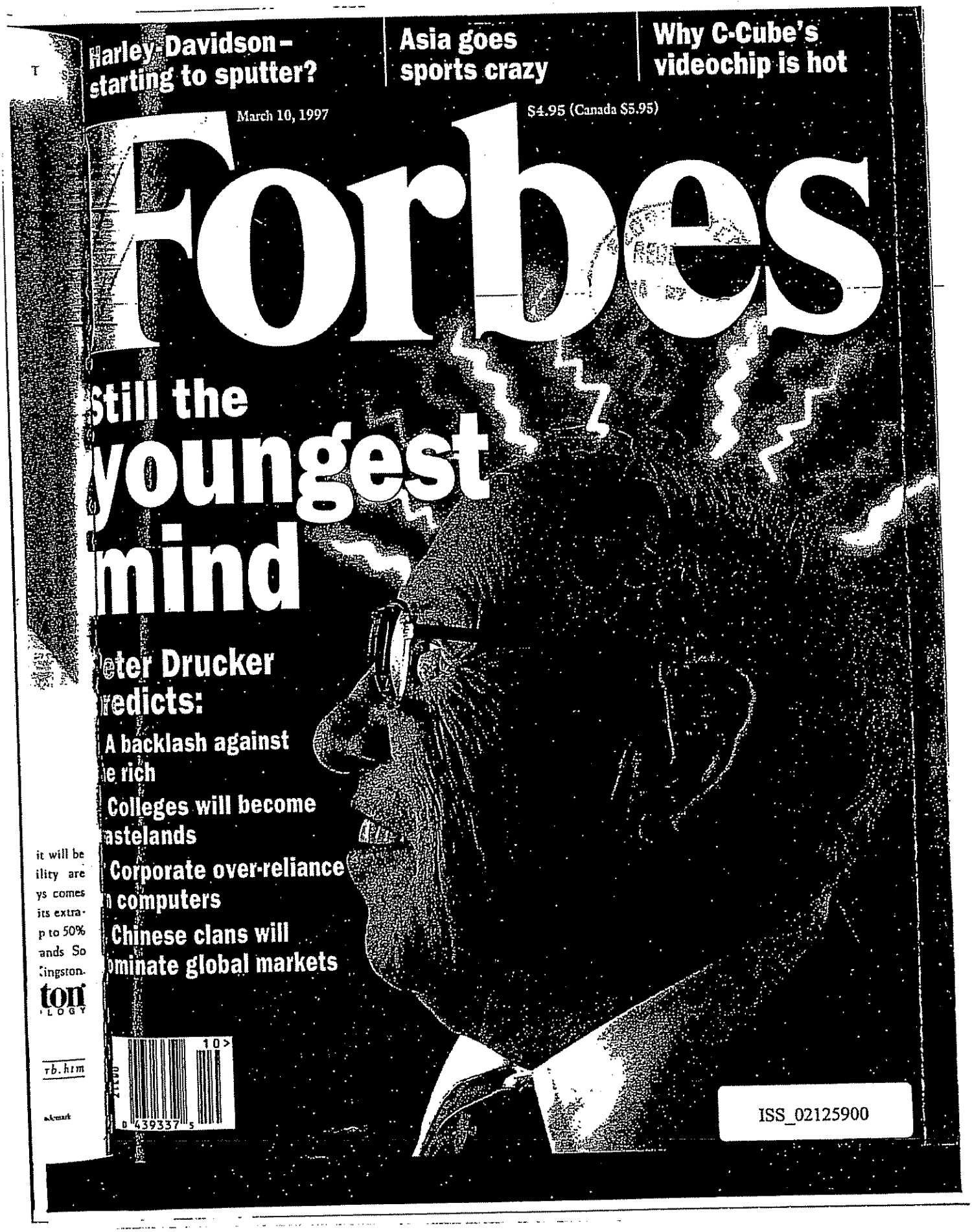
EXHIBIT O

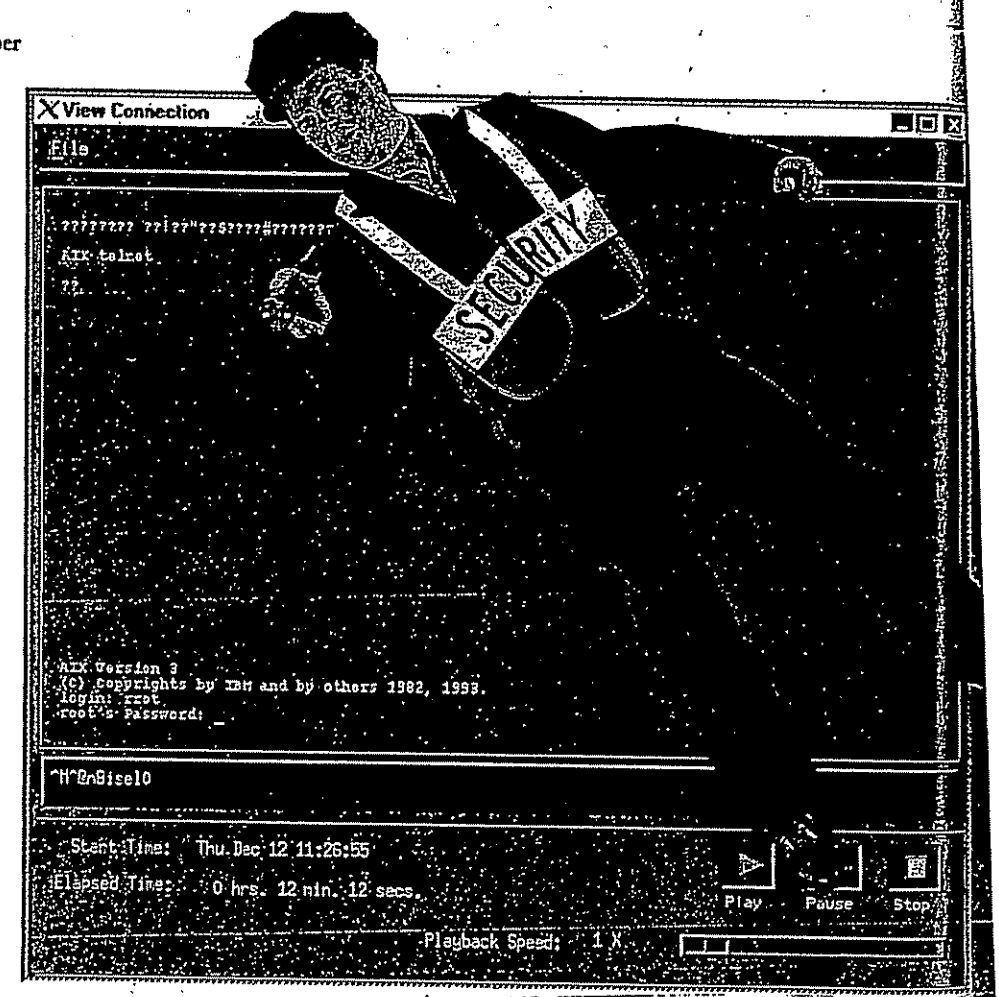

Harley-Davidson – starting to sputter?
Asia goes sports crazy
Why C-Cube's videochip is hot
March 10, 1997
$4.95 (Canada $5.95)
Forbes
Still the youngest mind
eter Drucker redicts:
A backlash against e rich
Colleges will become astelands
Corporate over-reliance computers
Chinese clans will ominate global markets
it will be ility are ys comes its extra- p to 50% ands So ingston.
ton LOGY
rb.htm
ademark
ISS_02125900

TECHNOLOGY
SILICON STARTUPS

Do you need a security guard to protect your data? Consider hiring an experienced break-in artist.

Cybercops

By Zina Moukheiber



Internet Security Systems founder Chris Klaus **He wanted to beat the bad guys.**

In William Gibson's 1984 science fiction bestseller, *Neuromancer*, digirobbers break into the cyberspace matrix and steal precious data. Christopher Klaus was a ninth-grader at Sarasota (Fla.) High School when he read that book. He was captivated. Why not play data cops and robbers for real?

In the summer of 1990 Klaus was one of 50 high school students to win internships at Lawrence Livermore National Laboratories in Livermore, Calif. There, dabbling on supercomputers connected to the Internet, Klaus started to develop hacker counterattack weapons. The idea: Find the weak spots in a corporate or university network. Stage a test break-in. Then educate the victim about how to plug the holes in its defense.

Klaus enrolled at Georgia Tech. Then he did a Bill Gates, dropping out in his sophomore year to start a software firm. He wrote 50,000 lines of C programming code.

In the novel the good guys use a weapon called Intrusion Countermeasures Electronics. Klaus called his firm Internet Security Systems, with an acronym reminiscent of the sci-fi: ICE. ISS is no Microsoft, not yet.

anyway, but it's doing pretty well for a firm that is only three years old and is run by a 23-year-old. Based in Atlanta, ISS probably did at least $10 million in sales last year from its network security auditing and monitoring software. Its clients include Intel, J.C. Penney, Merck, U.S. Bancorp, the National Aeronautics & Space Administration and the Pentagon.

Joe Morris, a network security expert at Bell Atlantic, is an ISS fan. He once needed some of his colleagues' computer addresses when he was calling from out of town. While they were boasting about how great their security was, Morris used an ISS scanner to grab a confidential address file off their server. "It took five minutes; I said don't bother anymore, I already have the file," says Morris. His colleagues at Bell Atlantic became quite agitated.

How did the scanner sneak in? Through a back door that, in Unix servers, is all too often left unlocked: the so-called Trivial File Transfer Protocol. This protocol can allow anyone on a computer network or on the Internet to transfer files without having to use a password. Sounds hard to believe, but when the procedure was written in the 1970s, programmers didn't have hackers in mind. Solution: Turn off this protocol.

Klaus' scanning software has 200 other hacker tricks where this one came from. It also has a library of 25,000 words and names that are likely to be used as passwords. Thought you were being clever to use your dog's name as a password? "Spot" is on the list. So are "Steelers," "eagerbeaver" and "Startrek." You're supposed to select a string of gibberish characters as your password, of course. But all it takes in a 400-terminal network is one dimwit with an easy password, and the hacker can get in.

One of the easiest points of entry into a network is through E-mail. This is after cracking open a password, or in lieu of it. The ISS scanner identifies the E-mail server and then figures out what software it is running. If it's running Unix's Sendmail version 8.6.5, cracking open the mail server is almost as easy as booting up. A real hacker would use the mail server to read or delete E-mail, and even to break into other servers by installing a piece of software that captures passwords on the network.

The ISS program sends a warning flag. Scanning can take anywhere from five minutes to a month, depending on the number of computers and routers (network transfer points) being tested.

You thought you were protected by an Internet fire wall? You might be, you might not. "A fire wall is about as intelligent as a hammer," says Alan Witty, a senior manager in information security at KPMG Peat Marwick. "It is dependent on the people who put it in place."

"We complement fire walls," says Klaus. "We make sure all the windows are closed and the doors are locked."

In case the house gets too stuffy, you can relax the rules a bit and then use Internet Security Systems' monitoring software. It acts like a camera inside a network of up to 50 computers. The administrator can thus keep a log on all transactions and look for suspicious activity.

Novell was the first to license Klaus' scanner, for $20,000—a number Klaus picked out of thin air. "I didn't even know what an invoice was," he shrugs. "They didn't teach me that one at Georgia Tech." But he knew he needed a manager. He hired Thomas Noonan, now 36, a Georgia Tech graduate who was working at Dun & Bradstreet Software and was ready to trade in his Brooks Brothers suits. After two rounds of venture financing, the two of them still own just over half of ISS.

They made their first sales call together in 1995. NASA invited Klaus to lecture on security. Afterward a colonel ushered them into a computer room, where he asked to see a demo of Klaus' software. A few minutes into the demo an alarm went off. The scanner had broken into the classified Jet Propulsion Laboratory and pulled a bunch of passwords. "They'd spent $1 million trying to secure their computers," says Noonan, who grabbed his laptop to prepare a price list. Current prices: $10 to $80 per computer for the scanner, depending on how many computers are on your network. The monitor costs $5,000.

The 75 employees of ISS work hard to discover chinks in fire walls before the hackers do. The latest: A way to crack into a Windows NT server through port 135. Microsoft has scrambled to issue a corrective patch. If you are not sure whether your system administrator remembered to install the patch, better get a scanner.

ISS president Tom Noonan
His easiest sale: to a classified government lab, after the ISS scanner broke in and stole passwords.

ANN STATES / SABA DIGITAL IMAGING FORBES